CLAIMS

What is claimed is:

1. A machine readable medium that provides instructions, which when executed by at least one processor, cause said processor to perform operations comprising:

encrypting a payload of a data block of a data-stream with at least one key, before transmitting the data-stream from a first system to a second system;

replacing a portion of said payload with a tag that identifies an at least one decrypting key to said first system, before said transmitting; and

setting a flag in a header of the data block that indicates that said payload has said tag, before said transmitting.

2. The medium defined in claim 1 wherein said encrypting includes encrypting said portion of said payload.

3. The medium defined in claim 1 wherein said tag includes one of:

a data-stream identifier, and

a data-stream identifier and a source, said source characterized by at least one of a source of said keys, and a source of said keys and a source of said portion of said payload.

4. The medium defined in claim 1 wherein said operations further include

receiving a transmission from said second system that includes data indicating said tag; and

sending one of said keys, and said keys and said portion of said payload, to said second system based on said transmission.

5. The medium defined in claim 1 wherein said operations further include before setting said flag and encrypting said payload; said first system

setting said flag in said header,

encrypting said payload, and

receiving a stream of data from a third system wherein said data-stream is based on said stream of data.

6. A machine readable medium that provides instructions, which when executed by at least one processor, cause said processor to perform operations comprising:

after a fixed-length data block of a data-stream, the data block having both a payload including an encrypted data portion and at least one tag bits, and a header, is received by a second system, reading a flag in the header indicating that the data block has the tag bits;

if the flag indicates that the data block has the tag bits, reading at least one bit identifying the data-stream in the tag bits;

sending a datum from the second system to a transmitting first system indicating an identification of the read data-stream based on the at least one bit;

the second system receiving from the first system a definition of a decrypting keys for the data-stream based on the datum sent from the second system to the first system; and

decrypting the data block in the second system based on the decrypting keys received by the second system.

7. The medium defined in claim 6 further including the second system receiving from the first system the portion of the payload based on the datum sent from the second system to the first system.

8. The medium defined in claim 6 further including the second system replacing the at least one tag bits in the payload with the portion of the payload, and if the portion of the payload is encrypted the decrypting includes decrypting the portion of the payload.

9. A method comprising:

a sending system replacing a portion of a data block payload with at least one tag bits that identify an at least one decrypting key;

said sending system setting a flag in a header of said data block that indicates at least one of said payload is encrypted and said payload includes said tag;

said sending system encrypting said payload with at least one key; and

said sending system transmitting said data block to a receiving system after said setting a flag, said encrypting, and said replacing.

10. The method defined in claim 9 wherein said encrypting includes encrypting said payload portion.

11. The method defined in claim 9 further including said sending system transferring a first data characterized by at least one of:

said at least one key to said receiving system; and

said at least one key and said payload portion to said receiving system.

12. The method defined in claim 11 wherein said sending system transmitting said first data is based upon said receiving system transmitting to said sending system said tag bits.

13. The method defined in claim 12 further including one of:

said sending system transmitting said payload portion to said receiving system based upon said receiving system transmitting to said sending system said tag bits; and said receiving system replacing said tag bits with said payload portion in response to receiving said payload portion from said sending system, and wherein said encrypting includes encrypting said payload portion, and said decrypting includes decrypting said payload portion; and

said sending system transmitting said payload portion to said receiving system based upon said receiving system transmitting to said sending system a first datum that identifies a data-stream that includes said data block, and said receiving system replacing said payload portion in response to receiving said payload portion from said sending system.

14. The method defined in claim 9 wherein said transmitting occurs via a shared memory unit.

15. The method defined in claim 9 wherein

said sending system and said receiving system are separate physical devices;

said transmitting of said data block occurs on a first channel; and

transmitting of non-data block data including at least one of said key from said sending system to said receiving system, said payload portion from said sending system to said receiving system, and a datum that identifies a data-stream that includes said data block, occurs on at least one separate second channel.

16. The method defined in claim 9 wherein said tag bits further identify a source of said keys in said sending system.

17. A method comprising:

a receiving system of an encrpted data block that has a payload and a header reading a set flag in a header of said data block;

said receiving system reading at least one tag bit in a payload portion of said data block in response to said reading said set flag;

said receiving system sending a first datum to a sending system of said encrypted data block that identifies a data-stream that includes said data block based on said read tag bits; and

said receiving system decrypting said a payload data of said payload portion in response to receiving a decryption keys from said sending system.

18. The method defined in claim 17 wherein said tag bits have a source identifier in said sending system of said decryption keys, and further including said receiving system sending said source identifier to said sending system in response to said reading.

19. A data safeguarding system for a data block sent from a first system to a second system including:

a first system payload replacement circuit that replaces a portion of a payload of said data block with a tag data that indicates at least one decryption key for said data block in said first system;

a first system header flag setting circuit that sets a flag in a header of said data block when said data block includes said tag;

a first system encryption circuit that encrypts said payload with said keys; and

a first system data-stream sending circuit that sends a data-stream that includes said data block to said second system after said header flag setting circuit sets said flag and said encryption circuit encrypts said payload and said payload replacement circuit replaces said portion of a payload.

20. The system defined in claim 19 wherein said first system encryption circuit encrypts said portion of said payload.

21. The system defined in claim 19 further including at least one of

a first system sending circuit that sends said at least one key to said second system; and

a first system sending circuit that sends said at least one key and said portion of said payload to said second system.

22. The system defined in claim 21 wherein said first system sending circuit sending is based upon said first system receiving from said second system a first datum that indicates at least one decryption key for said data block in said first system

23. The system defined in claim 19, further including:

a second system header flag reading circuit that reads said flag in said header;

a second system tag data reading circuit that reads said tag data if said second system header flag reading circuit indicates that said flag includes said tag data;

a second system data sending circuit that sends to said first system a datum that identifies said data-stream based on said tag data; and

a second system decrypting circuit that decrypts said encrypted block.

24. The system defined in claim 23 further including a first system key sending circuit that sends said at least one key to said second system, and wherein said second system decrypting circuit decrypts said data stream based on said at least one key.

25. The system defined in claim 23 further including

a first system sending circuit that sends said portion of said payload to said second system in response to receiving from said second system a datum that indicates said decryption keys in said first system

said first circuit encryption circuit further encrypts said replaced portion of said payload;

a second system payload replacement circuit that replaces said received tag data with said portion of said payload; and

said second system decrypting circuit further decrypts said portion of said payload.

26. The system defined in claim 19 wherein at least one of:

said sending occurs via a shared memory; and

said first system and said second system are separate physical devices; said sending of said data-stream occurs on a first channel; and sending non-data-stream data including at least one of said at least one key, said portion of said payload, and said data-stream identifier occurs on a second channel.

27. The system defined in claim 23 wherein said tag data further has an identifier for accessing a first system unit that can send to said second system said keys.

28. The system defined in claim 19 further including before said first circuit header flag setting circuit setting said flag and said first circuit encryption circuit encrypting said payload, a second circuit receiving circuit that can receive a stream of data from a third system wherein said data-stream is based on said stream of data.

29. A system for safeguarding a data block of a data-streamsent from a first system to a second system comprising:

a second system header flag reading circuit that reads a flag in a header of said data block;

a second system tag data reading circuit that reads a data-stream identifier in a tag data of a payload portion of said block if said header flag reading circuit indicates that said flag includes said tag data; and

a second system data sending circuit that sends to said first system a first datum that identifies said data-stream based on said data-stream identifier.

30. The system defined in claim 29 further including a second system decrypting circuit that decrypts said data block.